Please replace the paragraph beginning on page 9, line 1 with the following paragraph:

In use, the ciphering processor receives a packet. An address for the packet is determined and a security context associated with the packet address is located when present. The located security context is then used to cipher the packet. Alternatively, when the security context is not present, a signal is provided to the host processor which then determines and stores a security context for the packet. Such a method shifts much of the packet processing requirements from the host processor to the ciphering processor in an efficient and cost effective manner.

IN THE CLAIMS

Please cancel Claims 1-18.

Please add Claims 19-33 as follows:

19. A system for ciphering data for transmission by a communication device, comprising:

a memory device having

a memory buffer;

a first access port connected to said memory buffer; and

a second access port connected to said memory buffer; and

a data processing processor connected to said first access port via a first bus;

a ciphering processor connected to said second access port via a second bus, wherein

said first access port and said second access port each provide mutually independent access to said memory buffer; said second bus is not connected to said first bus; said data processing processor is adapted to receive said data and provide said data to said memory buffer over said first bus; and said ciphering processor is adapted to

retrieve said data from said memory buffer over said second bus, generate ciphered data from said data, generate integrity check information for said ciphered data using said data and provide said ciphered data to said memory buffer over said second bus.

20. The system for ciphering data as claimed in claim 19, wherein said ciphering processor includes an encryption module for generating said ciphered data and a hashing module for generating said integrity check information.

21. The system for ciphering data as claimed in claim 19, wherein said ciphering processor includes an encryption module for generating said ciphered data and a message digesting module for generating said integrity check information.

22. The system for ciphering data as claimed in claim 20, wherein said encryption module includes a DES encryption module for performing one of DES and triple-DES encryption.

23. The system for ciphering data as claimed in claim 20, wherein said hashing module includes a HMAC hashing module for encoding said integrity check information within said ciphered data.

24. The system for ciphering data as claimed in claim 19, wherein said memory buffer comprises dual port random access memory.

25. The system for ciphering data as claimed in claim 19, wherein said data processing processor comprises a security module, said security module retrieves a security context from memory, said security context used in generating said ciphered data.

26. The system for ciphering data as claimed in claim 25, wherein said security module determines a security context relating to at least one of a source of said data and a destination for said ciphered data and stores said security context in said memory buffer, said security context stored being accessible by said ciphering processor.

27. The system for ciphering data as claimed in claim 26, wherein said data processing processor comprises a security address module, said security address module stores an address associated with said security context in said memory buffer, said address based on said at least one of said source of said data and said destination for said ciphered data.

28. The system for ciphering data as claimed in claim 25, wherein said security module provides an indication to said data processing processor when a security context is not present in said memory buffer.

29. The system for ciphering data as claimed in claim 19, wherein said data processing processor operates asynchronously to said ciphering processor.

30. The system for ciphering data as claimed in claim 29, wherein said data processing processor is clocked by a first clock source, said ciphering processor is clocked by a second clock source and said first clock source is asynchronous to said second clock source.

31. The system for ciphering data as claimed in claim 19, said system further comprising:

a first communications port at which said data is received; and

a second communications port over which said data processing processor transmits said ciphered data.